What is claimed is:

1. A system for managing network traffic exchanged with a proscribed application capable of taking evasive action, comprising:

a flow analyzer analyzing flow characteristics of network traffic comprising a multiplicity of transient packets each including a parameterized header, comprising:

a parser retrieving operational characteristics from the parameterized header of each such transient packet generated by a plurality of intercommunicating applications;

a comparator identifying a proscribed application by comparing the operational characteristics to stored characteristics unique to the proscribed application; and

a flow monitor controlling transmission of each such transient packet subsequently exchanged with the proscribed application.

2. A system according to Claim 1, further comprising:

a classifier classifying a connection to the proscribed application by examining connection initialization operational characteristics.

3. A system according to Claim 1, further comprising:

a classifier classifying a login to the proscribed application by examining session initiation operational characteristics.

4. A system according to Claim 1, further comprising:

a classifier classifying a raw data flow to the proscribed application by examining data flow operational characteristics.

5. A system according to Claim 1, further comprising:

a traffic manager incrementally restricting bandwidth allocated to the network traffic specifically exchanged with the proscribed application until an evasive action is detected.

6. A system according to Claim 5, further comprising:

a bandwidth restriction store recording a bandwidth restriction threshold at which the evasive action by the proscribed application was triggered.

7. A system according to Claim 5, further comprising:

the traffic manager relaxing the bandwidth allocated to the network traffic specifically exchanged with the proscribed application by at least one increment responsive to the evasive action.

8. A system according to Claim 1, wherein the operational characteristics comprise at least one of a network address, port and traffic direction flow.

9. A system according to Claim 1, wherein the transient packets are communicated via the TCP/IP protocol.

10. A method for managing network traffic exchanged with a proscribed application capable of taking evasive action, comprising:

analyzing flow characteristics of network traffic comprising a multiplicity of transient packets each including a parameterized header, comprising:

retrieving operational characteristics from the parameterized header of each such transient packet generated by a plurality of intercommunicating applications;

identifying a proscribed application by comparing the operational characteristics to stored characteristics unique to the proscribed application; and

controlling transmission of each such transient packet subsequently exchanged with the proscribed application.

11. A method according to Claim 10, further comprising:

classifying a connection to the proscribed application by examining connection initialization operational characteristics.

12. A method according to Claim 10, further comprising:

classifying a login to the proscribed application by examining session initiation operational characteristics.

13. A method according to Claim 10, further comprising:

classifying a raw data flow to the proscribed application by examining data flow operational characteristics.

14. A method according to Claim 10, further comprising:

incrementally restricting bandwidth allocated to the network traffic specifically exchanged with the proscribed application until an evasive action is detected.

15. A method according to Claim 14, further comprising:

recording a bandwidth restriction threshold at which the evasive action by the proscribed application was triggered.

16. A method according to Claim 14, further comprising:

relaxing the bandwidth allocated to the network traffic specifically exchanged with the proscribed application by at least one increment responsive to the evasive action.

17. A method according to Claim 10, wherein the operational characteristics comprise at least one of a network address, port and traffic direction flow.

18. A method according to Claim 10, wherein the transient packets are communicated via the TCP/IP protocol.

19. A computer-readable storage medium holding code for performing the method according to Claims 10, 11, 12, 13, 14, 15, 16 and 17.

20. A system for dynamically controlling a rogue application through incremental bandwidth restrictions, comprising:

a flow monitor monitoring a network connection supporting a flow of network traffic in a distributed computing environment, the network traffic flow comprising a stream of data packets generated by a rogue application and incrementally adjusting bandwidth allocated to the monitored network connection

until the flow of the network traffic for the rogue application achieves a steady state of bandwidth restriction; and

a traffic manager controlling the flow of subsequent network traffic over the monitored network connection at the steady state of bandwidth restriction.

21. A system according to Claim 20, further comprising:

the flow monitor decreasing the bandwidth allocated to the monitored network connection for each new flow of network traffic until an evasive action by the rogue application is detected.

22. A system according to Claim 21, further comprising:

the flow monitor increasing the bandwidth allocated to the monitored network connection for a subsequent new flow of network traffic responsive to the evasive action.

23. A system according to Claim 20, further comprising:

the flow monitor storing the steady state of bandwidth restriction as a retrievable traffic flow control.

24. A system according to Claim 20, further comprising:

a flow analyzer identifying evasive action or other form of negative response taken by the rogue application.

25. A system according to Claim 20, further comprising:

a flow analyzer examining at least one of a network address, port and characteristics stored as parameters in a header of each such packet.

26. A system according to Claim 20, further comprising:

the flow monitor monitoring a redirected packet flow facilitated by the rogue application.

27. A system according to Claim 20, wherein the steady state of bandwidth restriction is sufficient to not trigger evasive action or other form of negative response by the rogue application.

28. A system according to Claim 20, wherein the rogue application executes in compliance with the TCP/IP protocol.

29. A method for dynamically controlling a rogue application through incremental bandwidth restrictions, comprising:

monitoring a network connection supporting a flow of network traffic in a distributed computing environment, the network traffic flow comprising a stream of data packets generated by a rogue application;

incrementally adjusting bandwidth allocated to the monitored network connection until the flow of the network traffic for the rogue application achieves a steady state of bandwidth restriction; and

controlling the flow of subsequent network traffic over the monitored network connection at the steady state of bandwidth restriction.

30. A method according to Claim 29, further comprising:

decreasing the bandwidth allocated to the monitored network connection for each new flow of network traffic until an evasive action by the rogue application is detected.

31. A method according to Claim 30, further comprising:

increasing the bandwidth allocated to the monitored network connection for a subsequent new flow of network traffic responsive to the evasive action.

32. A method according to Claim 29, further comprising:

storing the steady state of bandwidth restriction as a retrievable traffic flow control.

33. A method according to Claim 29, further comprising:

identifying evasive action or other form of negative response taken by the rogue application.

34. A method according to Claim 29, further comprising:

examining at least one of a network address, port and characteristics stored as parameters in a header of each such packet.

35. A method according to Claim 29, further comprising:

monitoring a redirected packet flow facilitated by the rogue application.

36. A method according to Claim 29, wherein the steady state of bandwidth restriction is sufficient to not trigger evasive action or other form of negative response by the rogue application.

37. A method according to Claim 29, wherein the rogue application executes in compliance with the TCP/IP protocol.

38. A computer-readable storage medium holding code for performing the method according to Claims 29, 30, 31, 32, 33 and 34.